State of California
Department of Technology Services

DTS Bulletin

Owner: Security Management Division
Midrange Database Support Unit

Number: 3132
Issue Date: 04/10/2009
Revised:

MIDRANGE DATABASE SERVER SECURITY STANDARD

Section 1 – Introduction

This Bulletin addresses the security requirements surrounding data access and administrator roles and responsibilities of Department of Technology Services (DTS) database administration. This Bulletin is applicable to DTS staff supporting Relational Database Management System (RDBMS) servers and DTS customers implementing RDBMSs in managed solutions.

Security is a major concern for modern-age systems, network, and database administrators. While it is natural for an administrator to be concerned about hackers and external attacks while implementing security, it is essential to first implement security within an organization by creating a security plan. Primarily, a security plan must identify which individuals of an organization will have access to data, the type of access that will be granted, and which database activities will be performed and by whom.

To access data within a database, a user must pass through two stages of authentication; one at the operating system level, the other at the database level. These two stages are implemented using login names and user accounts respectively.

Section 2 – Requirements

The requirements listed below must be implemented to consolidate database security across DTS managed services. They are necessary for DTS database system administrators to properly support, administer, and audit the database systems.

1. Current and future RDBMS databases shall be created by DTS database system administrators.
2. RDBMS installations shall retain current security rights unless they contrast with DTS Security Policy and/or Standard. If any configuration is in conflict with current DTS Security Policy or Standard, a remediation of non-compliancy will need to be coordinated.
3. RDBMSs which support report generating/rendering services (i.e. Crystal Reports, SQL Server Report Services, etc.) that provide a hypertext transfer protocol (HTTP) based interface with outbound traffic must not be designated over port 80 from the database tier of the standard n-tier network architecture. Refer to DTS Bulletin 3117 – Network Architecture Standard for details regarding acceptable network architectures in the DTS hosting environment.
4. Access to database server settings will be restricted to DTS database system administrators. If specific changes are needed, customers must submit a Service Request requesting the change.

5. DTS database system administrators:
    a. Maintain operating system and security patch levels and health of the servers.
    b. Maintain system hardening configuration documentation in accordance with DTS Security Bulletins. Refer to DTS Bulletin 3126 – Server Security Standard and DTS Bulletin 3302 – Security Patch Management Standard.
    c. Are responsible for server access accounts. Only DTS database system administrators are authorized to change access levels.
    d. Are responsible for reviewing, providing recommendations of changes if needed, and scheduling database job scripts.
    e. Are responsible for service accounts and their respective access rights for the database management system.
6. Customers shall have permissions as listed below to their databases:
    a. Database owner (DBO) access or equivalent is provided for database maintenance purposes.
    b. Applications must have specific roles and/or user permissions as needed to perform application functions.
7. Customers with job scripts that require elevated permissions to execute must supply the script to DTS database system administrators.

Section 3 – Applicability and Exclusions

A. This standard applies to DTS systems hosted in either the managed care environment or customer managed service environment. Direct any questions regarding the applicability of this standard to the Security Management Division for clarification.

This Bulletin does ***not*** apply to Customer Owned Equipment Managed Service (COEMS) customers or development only environments within DTS managed services.

B. Exceptions to this standard must be documented and will be considered on a case-by-case basis. Requests for an exception to this standard must be submitted via the DTS Security Policy/Bulletin Exception Request Form, DTS 358.

Section 4 – Auditing and Reporting

A. Auditing may be performed on a periodic or random basis by the Security Management Division or its designees. In the event an audit determines this standard is not being applied, notification will be sent to the appropriate person for remediation.

B. Any known violations of this standard must be reported to the DTS Chief Information Security Officer and the reporting employee's immediate supervisor.

Section 5 – Authority/References

Please contact your DTS Customer Representative for documents listed in this Bulletin not provided on the service catalog.

3400 - Acceptable Use Policy
3117 – Network Architecture Standard
3126 – Server Security Standard
3302 – Security Patch Management Standard
Security Policy/Bulletin Exception Request Form, DTS 358